IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF TEXAS

IN RE APPLICATION OF THE UNITED STATES FOR HISTORICAL CELL SITE DATA	)	Magistrate No. H-10-998M Magistrate No. H-10-990M Magistrate No. H-10-981MF

BRIEF OF AMICUS CURIAE SUSAN FREIWALD IN OPPOSITION TO THE GOVERNMENT'S REQUEST FOR REVIEW

Susan Freiwald
Professor of Law
University of San Francisco School of Law
2130 Fulton Street
San Francisco, CA 94117
(415) 422-6467
(415) 422-6433

TABLE OF CONTENTS

Statement of Interest 1

Summary of Argument 1

Argument 2

I. Government Acquisition of Location Information Is a Search Under The Fourth Amendment 2

A. Subjective Expectations of Privacy in Location Data 2

B. Objective Expectations of Privacy 4

C. Acquiring Location Data Must be Subject to the Warrant Requirement Because It Is Hidden, Continuous, Indiscriminate and Intrusive 6

II. The Government Does Not Advance a Compelling Reason Not to View Acquisition of Location Data as a Search 9

A. Location Data is Sufficiently Precise to Implicate the Fourth Amendment 9

B. A "Third Party Rule" Does Not Govern Acquisition of Location Data 12

C. Disclosure of Location Data May Not be Compelled Without A Warrant 17

III. Judge Smith Did not Abuse His Discretion in denying the Applications 20

A. Consulting Sources Beyond the Government's Submission Was Not Error 20

B. The Government's Affidavit Does Not Undermine Judge Smith's Ruling 22

Conclusion 26

TABLE OF AUTHORITIES

Cases

Berger v. New York, 388 U.S. 41 (1967) 6, 7
City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010) 5
Hardy v. Johns-Manville Sales Corp., 681 F.2d 334 (5th Cir. 1982) 21
In re Application of the United States of America for Historical Cell Site Data, 2010 WL 4286365 (S.D. Tex. Oct. 29th, 2010) ..... passim
In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 534 F. Supp. 2d 585 (W.D. Pa. 2008) 6, 7, 22
In re Applications of the United States, 509 F. Supp. 2d 76 (D. Mass 2007) 22
In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., 15 FCC Rcd. 17442 (2000) 22
In the Matter of the Application of the United States For And [sic] Order: (1) Authorizing Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services, 2010 WL 3021950 (W.D. Tex. 2010) 25
In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 311 (3rd Cir. 2010) ..... passim
In the Matter of the Application of the United States of America, 515 F. Supp.2d 325 (E.D.N.Y. 2007) 10
Katz v. United States, 389 U.S. 347 (1967) ..... passim
Kyllo v. United States, 533 U.S. 27 (2001) 2, 5, 11, 26
Old Chief v. United States, 519 U.S. 172 (1997) 20
Smith v. Maryland, 442 U.S. 735 (1979) 12, 13, 14, 24
United States v. Benford, 2010 WL 1266507, *1 (N.D. Ind. Mar. 26, 2010) 25
United States v. Forest, 355 U.S. 942 (6th Cir. 2004) 10
United States v. Forrester, 512 F.3d at 500 (9th Cir. 2008) 14
United States v. Karo, 468 U.S. 705 (1984) ..... passim
United States v. Knotts, 460 U.S. 276 (1983) 9, 10
United States v. Long, 64 M.J. 57 (C.A.A.F. 2006) 16
United States v. Maynard, 615 F.3d 544, 561-62 (D.C. Cir. 2010) 14
United States v. Miller, 425 U.S. 435 (1976), ... 12, 13, 15, 16
United States v. Torres, 751 F.2d 875 (7th Cir. 1984) 6
United States v. Warshak, 2010 WL 5071766 (6th Cir. 2010) ..... passim
United States v. White, 401 U.S. 745, 786 (1971) 4
Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), *vacated on ripeness grounds*, 532 F.3d 521 (6th Cir. 2008) (en banc) 18

Statutes

18 U.S.C. § 2518(7) 3
18 U.S.C. § 2703(f) 23
18 U.S.C. §2703(d) 17, 24

Other Authorities

Al Gidari, Jr., *Symposium: Companies Caught in the Middle,* 41 U.S.F. L. Rev. 535 (2007) 8, 26
Brief of Amicus Curiae Susan Freiwald in Support of Affirmance, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), ... 13
Catherine Crump and Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, 88 Crim. L. Reporter 1, 3 (2010) 23
CTIA Semi-Annual Wireless Industry Survey, (available at http://files.ctia.org/pdf/CTIA_Survey_Midyear_2010_Graphics.pdf) 5
Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev 112 (2007) 3
Hearing on Elec. Commc'ns Privacy Act Reform & the Revolution in Location Based Techs. & Servs. Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties, S. Comm. on the Judiciary, 111th Cong. (June 24, 2010), (Written Testimony of Professor Matt Blaze) 25
James X. Dempsey, *Digital Search and Seizure: Updating Privacy Protections to Keep Pace With Technology,* PLI Order No. 14648 (June-July 2008) 10
Jennifer King and Chris Jay Hoofnagle, Research Report*: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information* (April 18, 2008) 3
Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 165 (2008) 15, 19
Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash., L. Rev. 1375, 1397-1413 (2004) 19
Susan Freiwald, *First Principles of Communications Privacy*, Stanford J. Law & Tech. 2007 13
Susan Freiwald*, Online Surveillance: Remembering the Lessons of the Wiretap Act,* 56 Ala. L. Rev. 9 (2004) 6

STATEMENT OF INTEREST

Amicus is a law professor who teaches and writes scholarship in the areas of Cyberspace Law and Information Privacy Law. She has written several law review articles on how the Fourth Amendment and the federal surveillance statutes should apply to new communications technologies. She has also submitted amicus briefs in cases addressing the Fourth Amendment's application to newly emerging electronic surveillance techniques including in the Sixth Circuit regarding the Fourth Amendment protection of stored email. Amicus submitted amicus briefs in the Western District of Pennsylvania and the Third Circuit addressing the Fourth Amendment protection of location data. Amicus has no stake in the outcome of this case, but is interested in ensuring that electronic privacy law develops with due regard for the vital role electronic communications play in our lives.

SUMMARY OF ARGUMENT

Government acquisition of historical cell-site records ("location data" or "location information") constitutes a Fourth Amendment search because it intrudes upon users' reasonable expectations of privacy. That third-party cell-phone providers store location data does not detract from those expectations of privacy, contrary to the government's claim of a broad "third-party" rule. This court should reject the government's claim that the location information it seeks in its applications is insufficiently precise to implicate the Fourth Amendment. *See* Government's Memorandum of Law in Support of Request for Review at 27-30 (12/3/2010) (hereinafter "Gov. Brief"). To deny Fourth Amendment protection based on the government's assurance that it seeks only limited location data flouts the fundamental principle that Fourth Amendment protections may not be left in the hands of law enforcement agents. Because the

government claims the ability to acquire location data without first procuring a warrant based on probable cause, this Court should affirm Magistrate Judge Smith's denial of the government's applications. *See In re Application of the United States of America for Historical Cell Site Data*, 2010 WL 4286365 (S.D. Tex. Oct. 29th, 2010) ("*Smith Order*").

ARGUMENT

I. GOVERNMENT ACQUISITION OF LOCATION INFORMATION IS A SEARCH UNDER THE FOURTH AMENDMENT

When the "government violates a subjective expectation of privacy that society recognizes as reasonable," it conducts a Fourth Amendment search. *Kyllo v .United States*, 533 U.S. 27, 33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967). Because government agents intrude upon a cell phone user's reasonable expectation of privacy when they acquire his location data, they conduct a search under the Fourth Amendment and must either obtain a warrant based on probable cause or establish an exception to the warrant requirement. Common uses of cell phone technology support a subjective expectation of privacy in location data and applicable precedents support an objective expectation. Location data acquisition, like other forms of electronic surveillance, is hidden, continuous, indiscriminate and intrusive in ways that require extensive judicial supervision to protect Fourth Amendment rights.

A. Subjective Expectations of Privacy in Location Data

Most cell phone users would be unpleasantly surprised, if not outraged, to learn that a law enforcement agent could gain access to their location data without first obtaining a warrant based on a showing of probable cause. Location data provides a virtual map of a person's activities. It may divulge when and where a user gave confession, viewed an X-rated movie, or protested at a political rally. *See Smith Order*, slip op. at 20 (describing location data sought by the

government as providing "not a single snapshot at a point in time, but a continuous reality TV show, exposing two months' worth of a person's movements, activities and associations in relentless detail.") Knowledge that the government could keep track of such information could easily inhibit valuable and constitutionally protected activities.[1]

Not surprisingly, cell phone users regard access to their location information as yielding data about their locations. A recent study found that 73% of cell phone users surveyed favored "a law that required the police to convince a judge that a crime has been committed before obtaining [historical] location information from the cell phone company."[2] 72% also supported a law requiring the police to give notice to the user whose location data they seek before obtaining historical location information.[3] Both findings demonstrate that most users view their location data as private information and expect it to remain private absent a compelling need for access.[4]

People surely entertain a subjective expectation of privacy in their location data, and would not expect police to have access to it without first demonstrating a compelling justification to a reviewing court. *See United States v. Karo*, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part) ("As a general matter, the private citizen is entitled to

---

[1] In addition to implicating Fourth Amendment interests, location data disclosure may implicate First Amendment rights of expression and association. *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev 112 (2007) (identifying implications of electronic surveillance for First Amendment interests).

[2] Jennifer King and Chris Jay Hoofnagle, Research Report*: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information* (April 18, 2008) (available at SSRN http://ssrn.com/abstract=1137988).

[3] *Id.*

[4] 83% of respondents agreed that police should be able to track them in an emergency, a view which statutes reflect. *See, e.g.*, 18 U.S.C. § 2518(7) (providing a 48 hour period during which agents may wiretap without a warrant in an emergency).

assume, and in fact does assume, that his possessions are not infected with concealed electronic devices."). For the same reasons that people expect a law enforcement agent to obtain a warrant from a neutral magistrate before she may bug their conversations, monitor their phone calls or subject them to silent video surveillance, people would surely expect judicial oversight of that agent's use of their cell phones to track their every movement and activity.

B. Objective Expectations of Privacy

The objective prong of the reasonable expectation of privacy test ultimately requires this Court to make a normative finding about whether users should be entitled to view the object of the search as private. As Justice Harlan, author of the reasonable expectation of privacy test, explained: "The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risks of the electronic listener or observer without at least the protection of a warrant requirement." *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). The critical question in this case is whether in our society law enforcement agents may use cell phone technology as a window for constant surveillance of our citizens without the procedural limits imposed by the Fourth Amendment. The answer must be "no."

By analogy, the expectation of privacy users have in their location data must be objectively reasonable. Just as the Supreme Court recognized that warrantless government eavesdropping violated the privacy on which the target "justifiably relied" while using the telephone booth, *Katz v. United States*, 389 U.S. 347, 353 (1967), so warrantless access to location data would violate the privacy on which cell phone users justifiably rely while using their cell phones. When describing government acquisition of telephone conversations as a search under the Fourth Amendment, the Supreme Court in *Katz* reasoned that "[t]o read the

Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication," *Id.* at 352. To deny Fourth Amendment protection to location data would similarly ignore the vital role that mobile telephony has come to play today in the lives of the over 290 million subscribers in the United States.[5] *Cf. City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010) (assuming that user of a text messaging service had a reasonable expectation of privacy in his messages).

In the *Warshak* case, the Sixth Circuit employed a normative approach to determining reasonable expectations of privacy in new communications media that serves as a good model for this Court. In general, the court recognized that "[a]s some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise." *United States v. Warshak*, 2010 WL 5071766, *11 (6th Cir. 2010). As for email in particular, the court found that it "plays an indispensable part in the Information Age," *id*., and that it "requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve." *Id.*

The *Warshak* court's recognition that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish," *id*. at 10 (citing *Kyllo*, 533 U.S. 27, 34 (2001)), supports a finding of an objective expectation of privacy in location data.

[5] *CTIA Semi-Annual Wireless Industry Survey* at 2, (available at http://files.ctia.org/pdf/CTIA_Survey_Midyear_2010_Graphics.pdf) (reporting 292,847,098 cellular subscriber accounts in the U.S at the end of June 2010).

C. Acquiring Location Data Must be Subject to the Warrant Requirement Because It Is Hidden, Continuous, Indiscriminate and Intrusive

Location data acquisition shares those features of other types of electronic surveillance that the Supreme Court and lower courts have found to require high procedural hurdles and extensive judicial oversight. In *Berger*, the Supreme Court explained that electronic eavesdropping techniques presented "inherent dangers" and therefore required more "judicial supervision" and "protective procedures" than even "conventional" searches. *See Berger v. New York*, 388 U.S. 41, 60 (1967); *see also id.* at 64 (noting that New York statute permitting eavesdropping with insufficient judicial oversight constituted a "general warrant" in violation of the Fourth Amendment).[6] When they determined that the Fourth Amendment required the same procedural hurdles for use of silent video surveillance, several federal Courts of Appeal elaborated on which features necessitated heightened judicial oversight. Judge Posner, in a decision for the 7th Circuit whose reasoning was widely followed, explained that the *hidden, continuous, indiscriminate*, and *intrusive* nature of electronic surveillance raises the likelihood and ramifications of law enforcement abuse. *See United States v. Torres*, 751 F.2d 875, 882-84 (7th Cir. 1984); *see id.* at 882 ("[I]t is inarguable that television surveillance is exceedingly intrusive … and inherently indiscriminate, and that it could be grossly abused - to eliminate personal privacy as understood in modern western nations."); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 789-80 (2004) (discussing cases and requirements).

When government agents acquire location data they use a technique that is similarly hidden, continuous, indiscriminate and intrusive. Unlike the search of a home, which is usually

[6] In fact, law enforcement agents seeking location data should perhaps satisfy the heightened procedural requirements imposed on government wiretappers. *See Lenihan Order*, 534 F. Supp. 2d at 586 n.7

subject to view either by the occupant of the home or his neighbors, government acquisition of location data is *hidden*. Just as a telephone user does not know when a law enforcement agent wiretaps his call, a cell phone user does not know when a law enforcement agent acquires his location information. That significantly raises the risk that agents will exceed the scope of a proper investigation with impunity. In addition, location data reveals information over a *continuous* period, as do telephone conversations and video surveillance footage. The longer the period an investigation spans, the greater the likelihood that the government will conduct surveillance without sufficient justification. To address that risk, the Supreme Court required that electronic surveillance orders issue for a limited period of time, and cease as soon as the constitutional justification ceases. To apply for a renewal, agents must satisfy the same requirements as those imposed on initial requests. *See Berger*, 388 U.S. at 59. Because location data spans a period of time, 60 days in the applications here, its acquisition should also be subject to limits.

Besides being hidden and continuous, acquisition of location data is inherently *indiscriminate* in that much of the information obtained will not be incriminating. Just as the wiretapping of traditional telephone calls acquires non-incriminating conversations and video surveillance footage includes numerous innocent scenes, location data may reveal many movements and activities that are entirely unrelated to criminal actions.

For example, in the Third Circuit case, the government sought to compel the disclosure of location data for a user upon whom apparently no individualized suspicion had fallen. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 534 F. Supp. 2d 585, 588 & n.11 (W.D. Pa. 2008), *vacated and remanded*, 620 F.3d 304 (3rd Cir. 2010) (describing the subscriber whose location data agents sought as having a

cell phone apparently "used by" the target of the criminal investigation, but noting "no specific information connecting these two individuals.") (hereinafter "*Lenihan Order*"). The government appears to seek information about apparently innocent parties regularly. According to an industry lawyer, "With respect to location information of specific users, many orders now require disclosure of the location of all of the associates who called or made calls to a target." *See* Al Gidari, Jr., *Symposium: Companies Caught in the Middle, Keynote Address*, 41 U.S.F. L. Rev. 535, 557 (2007). The risk of acquiring information about non-incriminating activities mandates substantial judicial oversight to reduce unwarranted invasions of privacy and to ensure that searches not become government fishing expeditions.

As already discussed, law enforcement acquisition of location data has the potential to be extremely *intrusive* in that it may disclose a detailed record of the target's movements and activities.[7] Uninvited and virtually constant government observation of one's movements implicates constitutional privacy rights, the right to travel, and First Amendment rights of association and expression. Though location information differs from telephone conversations and videotaped footage, its acquisition shares the intrusive character of wiretapping and video surveillance. Because of that, it must be subject to heightened requirements, and at least a warrant, so that the government does not needlessly intrude on valuable privacy rights.

Importantly, law enforcement acquisition of historical location data can intrude into personal privacy even more than acquisition of real-time or prospective location information. A law enforcement agent seeking prospective location data could get an order on August 1 to track the target's movements for three months, but then would have to wait until October 31 to obtain three months of location data to review. Alternatively, the agent could ask the provider for

[7] In Part II.A. *infra*, I address the government's claim that acquisition of location data is insufficiently precise to intrude on constitutional privacy rights. *See* Gov. Br. at 27-29.

historical data and immediately obtain a year's worth or more of the target's location information.[8] The length of time the target's cell phone generates records and the service provider stores them set the only limit on the scope of the historical records the law enforcement agent may acquire.

As the preceding discussion shows, government acquisition of location data shares the same features of wiretapping, bugging and video surveillance that make those investigative methods particularly invasive and particularly subject to abuse. In recognition of that and as a matter of constitutional law, courts must impose on those agents who seek location data at least the warrant requirement, if not the same requirements as those imposed on agents seeking to wiretap or conduct video surveillance. Requiring that law enforcement agents demonstrate probable cause to a neutral magistrate before they may compel the disclosure of location data is the minimum constitutional safeguard.

II. THE GOVERNMENT DOES NOT ADVANCE A COMPELLING REASON NOT TO VIEW ACQUISITION OF LOCATION DATA AS A SEARCH

A. Location Data is Sufficiently Precise to Implicate the Fourth Amendment

In its brief, the government contends that the tracking device precedents of *United States v. Knotts*, 460 U.S. 276, 282 (1983) and *United States v. Karo*, 468 U.S. 705 (1984), preclude constitutional protection for location data. *See* Gov. Brief at 25-26. The government errs, however, because the *Knotts* case has little to say about location data, and the *Karo* case supports a Fourth Amendment claim in location information.

The *Knotts* Court found no reasonable expectation of privacy in movements on public roads. 460 U.S. at 281. *Knotts*, decided in 1983, addressed the government's monitoring of a

[8] Historical location information could contain data of quite recent vintage.

radio beeper attached to a large container of chemicals stored in an automobile that government agents followed "on public streets and highways." *Knotts*, 460 U.S. at 281. Agents had affixed a beeper to a five gallon drum of ether and monitored the drum rather than the individual suspects. If those surveillance targets had been separated from the drum for any reason, the monitoring would have ceased being effective. Cell phones, on the other hand, travel with and often on the users themselves. Modern cell phones include so many features, in addition to calling, that users have reason to have them at hand all the time. Thus the beeper monitoring the Supreme Court considered in *Knotts* was considerably less intrusive, by virtue of being considerably less reliable, than that afforded by acquisition of location data. *Cf. In the Matter of the Application of the United States of America*, 515 F. Supp.2d 325, 338 (E.D.N.Y. 2007) (observing that "the evolution of technology and the potential degree of intrusion changes the [Fourth Amendment] analysis"). In addition, the *Knotts* Court relied on the "diminished expectation of privacy in an automobile." *Knotts*, 460 U.S. at 281. Location data, in contrast, reveals the movements and activities of cell phone users in many places besides their cars; modern cell phones accompany their users on walks, into buildings, as well as into their homes.

The monitoring the police conducted in *Karo*, and which the Supreme Court found to implicate the Fourth Amendment, comes closer to acquisition of location data. The *Karo* Court found a violation of constitutional privacy rights when agents monitored the beeper in "a private residence, a location not open to visual surveillance." *Karo*, 468 U.S. at 714. The Court elaborated that agents determined that "the beeper was inside the house," which was "a fact that could not be visually verified." *Id.* at 715. The Court imposed Fourth Amendment constraints on the government's use of the beeper "to determine… whether a particular article – or a person, for that matter – is in an individual's home at a particular time." *Id.* at 716.

While it is not necessary for an investigative technique to penetrate the home to intrude upon a reasonable expectation of privacy, it is extremely likely that location data will reveal at least as much information about the inside of a home as the beeper revealed in *Karo*. With simple inferences, law enforcement agents may use even "imprecise" location data to reveal that a target is in his home, awake, and using the telephone.[9] *See, e.g.*, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 311 (3rd Cir. 2010)), *pet. for reh'g en banc denied* (3d Cir. Dec. 15, 2010) (hereinafter "*Third Circuit Opinion*") ("For example, historical [location data] could provide information tending to show that the cell phone user is generally at home from 7 p.m. until 7 a.m. the next morning."); *id*. at 311-12 (citing government testimony illustrating that "the government has asserted in other cases that a jury should rely on the accuracy of cell tower records to infer that an individual or at least her cell phone, was at home."). That evidence refutes the government's assertion that location data is insufficiently precise to implicate the Fourth Amendment. *See Kyllo*, 553 U.S. at 36 (rejecting "dissent's extraordinary assertion that anything learned through 'an inference' cannot be a search"). Location data acquisition is at least as intrusive, and likely much more so, than the information found subject to Fourth Amendment protection in *Karo*.

Even if agents could somehow know that the location data it sought would not reveal activities within the home, which it could not, government acquisition of location data still intrudes upon a reasonable expectation of privacy. Because cell phones typically travel in pockets or pocketbooks, they are "withdrawn from public view" under the Court's reasoning in *Karo*. 468 U.S. at 716. As the Supreme Court explained in that case, agents need to "obtain

[9] By "imprecise" location data, I refer to the location information generated only at the start and end of a cell phone call. However, I discuss in Part IIIB infra reasons why this Court should not limit its consideration to that subset of location data.

warrants prior to monitoring a beeper when it has been withdrawn from public view." *Id*. at 719. They similarly need to obtain a warrant before acquiring location data when the cell phone that produces it is removed from public view. As Justice Steven's explained in *Karo*: "The concealment of such [electronic devices] on personal property significantly compromises the owner's interest in privacy, by making it impossible to conceal that item's possession and location from the government, despite the fact that the Fourth Amendment protects the privacy interest in the location of personal property not exposed to public view." *Id*. at 735 (Stevens, J., concurring in part and dissenting in part).

B. A "Third Party Rule" Does Not Govern Acquisition of Location Data

Contrary to the government's claim, see Gov. Br. at 13-19, no "third party" rule excuses the government from the constitutional requirement of a warrant. The Sixth Circuit persuasively limited application of any "third party" rule in the recent *Warshak* case, 2010 WL 5071766, at *13, and the Third Circuit found it inapplicable to location data in its recent decision. *See Third Circuit Opinion*, 620 F.3d at 317-18. None of the government's arguments calls either persuasive precedent into question or provide a good reason to find that either *United States v. Miller*, 425 U.S. 435 (1976), or *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), governs location data.

Essentially, the government urges this court to find records containing location data analogous to the bank records that the Supreme Court found unprotected by the Fourth Amendment in *Miller*. *See* Gov. Brief at 13 (relying on *Miller* case). By characterizing location data as "business records held by a third-party," *id.*, the government presses for an analytical short-cut, by which some lower courts have reject constitutional protection for "third party records" without fully conducting an inquiry into reasonable expectations of privacy. *See*

generally, Susan Freiwald, *First Principles of Communications Privacy*, Stanford J. Law & Tech. 2007 (criticizing courts for using supposed third party rule to avoid reasonable expectations of privacy analysis.) The government also claims that *Smith v. Maryland* precludes Fourth Amendment protection for location information because users voluntarily convey it to service providers in the same way that telephone users conveyed telephone numbers to the phone companies in 1979. Gov. Brief at 14-19

The Third Circuit, which is the only federal appellate court to consider the Fourth Amendment regulation of location data, squarely rejected the application of both *Miller* and *Smith* to location data. *See Third Circuit Opinion*, 620 F. 3d at 317. The Third Circuit rejected that idea that a cell phone user "voluntarily expose[s]" his location data in the same way that he exposes the telephone numbers that he dials. *Id.* at 317-18. The government disputes that holding, without directly confronting it, by arguing that users voluntarily expose their location data because they are aware that it is generated. *See* Gov. Brief at 17 (establishing users' knowledge of location data generation and collection). Cell phone users are much less aware, however, of their providers' practices regarding location data. The government does not establish that cell phone customers realize that providers make permanent records of their location data because there is no evidence that subscribers ever see a listing of location data.[10] The government offers no provider-published information — analogous to the phone book excerpts in *Smith* — which would establish customer awareness of location data tracking and retention. That the government also argues users are *not* aware of the generation of location data

[10] In the Third Circuit case, the government's exemplar bore no markings of a customer communication, but instead looked like one page of a large report pulled from a database. *See* Brief of Amicus Curiae Susan Freiwald in Support of Affirmance at 18-19 , *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), *available at* http://www.usfca.edu/law/docs/freiwalds_uscourtappeals_brief.

undermines it claim of user awareness. *See* Gov. Brief at 15 ("Thus, it makes no difference if some users have never thought about how their cell phones work."). Ultimately, however, whatever awareness users have of the possibility that location data exists, they do not assume the risk that their location data will be disclosed to government agents without a warrant. *See Smith Order*, slip op. at 33. ("[T]he user has not 'knowingly exposed' or 'voluntarily conveyed' [location data] to the provider, as those phrases are ordinarily understood.")

Moreover, because location data reveals so much more information than the limited information conveyed by dialed telephone numbers, the *Smith* decision is inapposite. *See, e.g., United States v. Forrester*, 512 F.3d at 500, 510 (9th Cir. 2008) ("When the government obtains … IP addresses … it does not find out the contents of messages *or know the particular pages on the website the person viewed*.") (emphasis added); *see also id*. at 511 (specifically stating that its holding "does not imply that more intrusive techniques ... are also constitutionally identical to the use of a pen register."). As discussed above, location data is much closer to the GPS data that the D.C. Circuit viewed as not covered by *Smith v. Maryland* in the *Maynard* case. *See United States v. Maynard*, 615 F.3d 544, 561-62 (D.C. Cir. 2010), *pet. for reh'g en banc denied* (D.C. Cir. Nov. 19, 2010) (distinguishing *Smith v. Maryland* on the grounds that one does not constructively disclose to the public the "whole of one's movements over the course of a month because … that whole reveals far more than the individual movements it comprises.")

In a similar context, the Sixth Circuit rejected the government's argument that a "third party rule" defeats an email user's expectation of privacy. According to the *Warshak* panel, an email user does not convey his email to his service provider to be put "to use 'in the ordinary course of business.'" *Warshak*, 2010 WL 5071766, at *13. Instead, the service provider is a mere "intermediary, not the intended recipient of the emails," whose access does not defeat the user's

reasonable expectation of privacy. *See id*. (citing Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 165 (2008)). Similarly, a cell phone service provider is much more like an intermediary who processes location data in order to facilitate the cell phone user's communications with *other people*. Service providers are quite distinct from the bank in *Miller*, which the Supreme Court considered to be a party to the transactions with the defendant that generated the records. *See Miller*, 425 U.S. at 440-41 ("The records of respondent's accounts … pertain to transactions to which the Bank itself was a party.") The analogy that the Supreme Court drew between Miller's confiding in the Bank and a person confiding in his friends, *id.* at 443, does not describe the way in which location data is generated. *See Smith Order*, slip op. at 31 ("Cell site data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal.")

In fact, the *Warshak* panel reasoned that a user's consent to service provider access to provide a service does not forfeit a reasonable expectation vis-à-vis law enforcement access. Service provider access is sufficiently extensive "to snuff out a reasonable expectation of privacy" only in limited situations, such as when the provider "expresses an intention to 'audit, inspect and monitor' its subscriber's emails." *Warshak*, 2010 WL 5071766, at *13. Notably, the Sixth Circuit rejected a monolithic expectation of privacy that is defeated whenever the information at issue is seen by anyone. Instead, and appropriately, the court recognized that we may permit a service provider to run its business without relinquishing the protections of the warrant requirement: the interposition of a neutral magistrate to review the propriety and need for the government to pry into our personal communications.

Applying that approach to location data means that just because the service provider retains and has access to our location information does not mean that we waive a reasonable

expectation of privacy in that data vis-à-vis law enforcement access. As the government recognizes, service providers access users' location data to run their service. *See* Gov. Brief at 15 (describing how service providers "create [location data] records" for their "own business purposes"); *id*. at 17-18 (quoting T-Mobile Privacy Policy that states: "[w]e use personal information for a variety of business purposes…."). Permitting a service provider to access information to run its business does not imply consent to give up Fourth Amendment protections. *See, e.g., Warshak*, 2010 WL 5071766, at *12 ("[U]nder *Katz*, the degree of access granted to [the service provider] does not diminish the reasonableness of Warshak's trust in the privacy of his emails."); *United States v. Long*, 64 M.J. 57, 63 (C.A.A.F. 2006 ([c]onsent to monitoring did not imply consent to "engage in law enforcement intrusions . . . in a manner unrelated to the maintenance of the e-mail system.")

The government does not call into question the reasoning of either the Third or Sixth Circuit. Contrary to the government's contention, Gov. Brief at 19, constitutional protection is not strictly limited to "private" as opposed to "business" records. The Third Circuit made no preliminary finding that location data constitutes "private" papers when it rejected the *Miller* analogy, though the rich and detailed picture location data paints of one's activities certainly makes a reasonable expectation of privacy more justified. *See Third Circuit Opinion*, 620 F.3d at 317. Similarly, the *Warshak* panel made no finding that the emails at issue were stored in a private account, although it was impressed by how much private information was contained in the 27,000 emails that Warshak's service providers disclosed to the government pursuant to the warrantless orders in that case. *See Warshak* case, 2010 WL 5071766, at *10 (quoting from Warshak's brief that his emails contained "his entire *business* and personal life") (emphasis added).

Neither does constitutional protection depend on ownership, control or possession, contrary to the government's claim. *See* Gov. Brief at 13-16. Were it otherwise, the Supreme Court would have wrongly decided *Katz* because it held that bugging a public telephone booth implicated the Fourth Amendment even though it involved neither a physical trespass into the defendant's property nor acquisition of data in which the defendant could assert ownership, possession or control. *See Katz v. United States*, 389 U.S. 347 (1967). In the Third Circuit case, the target had no greater claim to ownership, possession or control of the records than the targets in the applications Judge Smith considered. Warshak himself stored emails on his service provider's servers and asserted no property rights in them.

Similarly, the constitutional question does not turn on whether subscribers are aware that their providers obtain cell phone location information. *See* Gov. Brief at 17. As the *Warshak* Court discussed, merely knowing that third parties have the capability to invade one's privacy does not constitute waiver of a privacy interest. *Warshak* case, 2010 WL 5071766, at *12 ("Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy"); *see also id*. at *13 ("[S]ome degree of routine access is hardly dispositive with respect to the privacy question.").

C. Disclosure of Location Data May Not be Compelled Without A Warrant

The government renews a remarkably circular argument that it made in the *Warshak* litigation when it contends that because a 18 U.S.C. §2703(d) order ("D order") may be used to compel disclosure of service provider records, and because a D order is more like a subpoena than a warrant, "a reasonableness standard rather than the warrant requirement" obtains in this case. Gov. Brief at 5. That statement begs a key question: does the Fourth Amendment permit the government to compel disclosure of the location data it seeks without first obtaining a

warrant based on probable cause? The answer to that question does not arise from a perusal of Congress' language, but rather from a reasonable expectation analysis of location data. *Cf. Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007*), vacated on ripeness grounds*, 532 F.3d 521 (6th Cir. 2008) (en banc) ("The government's compelled disclosure argument, while relevant, therefore begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-a-vis the party who is subject to compelled disclosure-in this instance, the ISPs.") According to the constitutional analysis, as I argued in Part I above, the Fourth Amendment requires a warrant for compelled disclosure of location data. Its acquisition intrudes upon reasonable expectations of privacy in a way that requires the interposition of a neutral magistrate to ensure that government investigators stay within constitutional limits.

A statutory provision that purports to permit the government to compel disclosure of location data with fewer procedural protections than those provided by a warrant is unconstitutional. That is just what Magistrate Judge Smith implied and that was an appropriate exercise of the judicial review power. *See Smith Order*, slip op. at 35. (denying the governments' requests for information under the authority of the Stored Communications Act ("SCA") because "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment.")

The Sixth Circuit ruled similarly just last month. After analyzing the nature of modern email and appreciating how intrusive it is for government to acquire it, the Sixth Circuit held that "it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment." *Warshak*, 2010 WL 5071766, at *12. The court elaborated that "if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search,

which necessitates compliance with the warrant requirement absent some exception." *Id*. After deciding the government agents violated the Fourth Amendment when they obtained his stored email using a D order instead of a warrant, the Court went on to state "[m]oreover, to the extent the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." *Id*. at *14.

Interestingly, the Sixth Circuit did not address the government's argument that statutory provisions authorizing compelled disclosures are not subject to the warrant requirement. *See* Government Brief to the Sixth Circuit, 2009 WL 3392997, at 106-109 (arguing that "the Fourth Amendment does not impose particularity, probable cause or notice requirements on compelled disclosures (as opposed to warrants).") Apparently the Sixth Circuit did not feel it necessary to point out that the decisions the government cited in which compelled disclosure (without notice, probable cause, or particularity) was permitted were those in which the target lacked a reasonable expectation of privacy under the approach of *Katz*. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 141-47 (2008) (discussing and rejecting government's compelled disclosure argument when users have a reasonable expectation of privacy); Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash., L. Rev. 1375, 1397-1413 (2004) (discussing compelled disclosure precedents). When the records at issue implicate a reasonable expectation of privacy, as location data does, the compelled disclosure argument falls away. *See Warshak*, 490 F.3d at 473 (explaining that if the user does not have a reasonable expectation of privacy in the data sought, the government may meet the reasonableness standard applicable to compelled disclosures, but if the user has a reasonable expectation of privacy, then the warrant requirement applies).

III. JUDGE SMITH DID NOT ABUSE HIS DISCRETION IN DENYING THE APPLICATIONS

A. Consulting Sources Beyond the Government's Submission Was Not Error

The government's complaint about Judge Smith's reliance on sources outside of the government's applications is misguided. I am unaware of any rules of evidence, and the government does not cite to any, that limit what a Magistrate Judge may consider when making a determination about whether a requested order for location data would run afoul of the Fourth Amendment if issued. A judge should be able to consider any evidence he considers relevant to a question that implicates his oath to abide by the Constitution to ensure he makes no rulings that violate it. Magistrate Judge Smith, as any federal judge, should be capable of determining the weight and persuasiveness of evidence he consults. That he gave the government the opportunity to furnish its own views on the evidence he intended to look at and to supplement that evidence demonstrates Judge Smith's procedural care. Tellingly, nowhere in its memorandum does the government actually assert that Judge Smith abused his discretion in considering the evidence he consulted. *Cf. Old Chief v. United States*, 519 U.S. 172, 183 n.7 (1997) (describing abuse of discretion standard for admissions of evidence claimed to be prejudicial).

The government's challenge to Judge Smith's approach seems all the more surprising given the ex parte nature of the proceeding. Judge Smith appropriately viewed the government as of limited assistance in answering the question whether its own application ran afoul of the Constitution. As this litigation illustrates, the government has a strong interest in convincing courts that it may obtain location data without a warrant. Government lawyers have pressed that position up through the Third Circuit in extensive briefing and oral argument.

The judicial notice doctrine, upon which the government relies heavily, rests on the concern that aggressive judicial fact-finding may circumvent a party's ability to contest the facts put forth by the other party in an adversarial setting. *See, e.g.*, *Hardy v. Johns-Manville Sales Corp.*, 681 F.2d 334, 347 (5th Cir. 1982) (appellate court rejected lower court's finding that "asbestos in all causes forms cancer," because it "burden[ed] [the] defendant's ability to present … evidence" that its products were not dangerous). In the ex parte hearing below, the government was the sole party with the opportunity to present its case, and ran no risk, therefore, that it would lack an opportunity to contest the other side's facts. Because Judge Smith gave the government notice of his intent to consult other sources and the opportunity to both present its own brief and comment on his proposed sources, it hardly appears that the government's ability to contest facts was constrained.

In particular, the government cries foul because Judge Smith did not inform them more specifically of the exact information he planned to cite before he issued his opinion. Gov. Brief at 2. That objection falls flat. That Judge Smith identified the sources he intended to consult was certainly sufficient to permit the government to consult those same sources and respond to them. The government further complains that Judge Smith did not make use of the government's belief, "[u]pon further inquiry," that providers do not record data when the cell phone is an idle state rather than engaged in a call. *See* Gov. Brief at 2 n.2. Such idle state data is also known as "registration data" because it is created when the cell phone registers with the cell tower periodically.[11] The government's failure to inform Judge Smith about its beliefs about location

[11] *See Lenihan Order*, 534 F. Supp. 2d at 590 (finding the registration data is produced every seven seconds); *see also In the Matter of the Application of the United States For And [sic] Order: (1) Authorizing Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services*, 2010 WL 3021950, *10 (W.D. Tex. 2010) (expressing concern that "receipt of

data until two months after it applied for that data, and in fact, until about five weeks after it had submitted a brief specifically designed to support the constitutionality of its application, falls squarely on the government and not Judge Smith.

While the government complains that Judge Smith's facts do not match facts found in earlier decisions including a three-year old magistrate decision and a ten-year old FCC decision, Gov. Brief at 9, Judge Smith cited both decisions in his opinion. *Smith Order*, slip. op. at 2 n.4 (citing *In re Applications of the United States*, 509 F. Supp. 2d 76 (D. Mass 2007); *id*., slip op. at 31 n. 94 (citing *In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.*,15 FCC Rcd. 17442 (2000)). Far from calling the credibility of the information Judge Smith relies on into question, his use of more recent information (from mid-2010) reflects that cell phone technology has changed over time and that location data was much different ten years ago. *See Smith Order*, slip op. at 31 ("[B]efore the advent of GPS and the current generation of network-based technology, it was not possible to locate cell phone users with any degree of precision."). Judge Smith's use of current rather than outdated information buttresses rather than detracts from the credibility of his decision.

B. The Government's Affidavit Does Not Undermine Judge Smith's Ruling

The government's belief about one of the provider's failure store to registration and duration data does not undermine Judge Smith's order. *See* Gov. Brief at 10. The government argues that Judge Smith should have "specifically reference[d] T-Mobile and MetroPCS" in his findings of fact since they were the providers whose records the government sought. Gov. Brief

---

[location data] will permit the government to 'follow' the phone user's movements 24 hours a day, 7 days a week, wherever they go, whatever they are doing.") (hereinafter "*Austin Opinion*").

at 11. Had Judge Smith done that, the government asserts, he would have known that MetroPCS does not currently store records related to cell phone locations when the phone is idle or during the duration of the call, in the normal course of business. Affidavit, ¶¶ 3, 8, 9.[12] Before discussing why MetroPCS' claims about its practices do not determine the constitutional question in this case, it bears noting that MetroPCS did not claim that it lacked capability to record such information. By its own terms, the affidavit does not apply "in response to a prospective court order." In other words, had the government requested that MetroPCS store registration or duration data, nothing in the affidavit suggests that MetroPCS would not or could not have done so. Records recently released pursuant to Freedom of Information Act requests reveal that government agents have sought and received "even the most precise cell tracking information" from various service providers. *See* Catherine Crump and Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, 88 Crim. L. Reporter 1, 3 (2010) (reporting that two U.S. Attorney's offices failed to obtain warrants for access to such precise location data, despite the Department of Justice's recommendation that they do so).

Government agents used a prospective court order in the *Warshak* case to obtain data that otherwise would not have been stored. As the Sixth Circuit described, agents used an 18 U.S.C. § 2703(f) order to request that the service provider preserve records prospectively.[13] The

[12] The Government asserts the T-Mobile's practices are similar to MetroPCS's, Gov. Brief At 10, but was apparently unable to secure an affidavit from the company to confirm that. Gov. Brief at 5 n.3. T-Mobile's own privacy policy alerts its subscribers that its "network detects your device' approximate location whenever it is turned on (subject to coverage limitations)." Gov. Brief At 18 (quoting from T-Mobile's privacy policy).

[13] The concurring judge viewed the use of a preservation order to retain records prospectively to be an end-run around the Wiretap Act and a constitutional violation. *Warshak*, 2010 WL 5071766, at *57. The decision did not address that question, perhaps because the majority

government requested stored email records that would not otherwise have been retained pursuant to D orders issued several months later. *Warshak*, 2010 WL 5071766, at *9. While Judge Smith made no mention of preservation orders in this case, the government's ability to use such orders to create fuller records, and its practice of doing so, reduces the relevance of MetroPCS's comments about its normal practices.

The government argues that Judge Smith's discussion of cell phone providers in general is problematic because it does not describe MetroPCS in particular. Gov. Brief at 11. This very case illustrates the prescience of the Supreme Court's comment that constitutional protection cannot depend on the record keeping practices of individual businesses. *See Smith v. Maryland*, 442 U.S. at 745 (noting that tying constitutional protection to the "billing practices of a private corporation" would make a "crazy quilt of the Fourth Amendment."). Here, the government's application indicated the distinct possibility that the providers from whom it sought location data would have both registration and duration data available. *See Smith Order*, slip op. at 1 ("[T]he Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not."). The Government has requested registration and duration data in several other cases including in the Third Circuit case. *See Third Circuit Opinion*, 620 F.3d at 308 (quoting application as seeking "without limitation . . . call handoffs, registrations and connection records."); *United States v. Benford*, 2010 WL 1266507, *1 (N.D. Ind. Mar. 26, 2010) (describing the information sought as data "identifying which cell tower communicated with the cell phone while it was turned on."); *Austin Opinion*, 2010 WL 3021950 at *8 (describing government's application as seeking "the exact location of the Target Devices

---

considered Warshak to have waived his Fourth Amendment claim regarding preservation. *Warshak*, 2010 WL 5071766, *15 n. 19.

(differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the third party Provider's infrastructure.)".

The question is not what one provider purportedly records, but rather what information is available from some of the thousands of providers of cellular phone service. As Matt Blaze testified at Congress, the trend should be towards more collection of data as the cost of storage continues to decrease and companies conceive of more ways to make money off of the data, either by using it to hone the provision of services or in the provision of related services or marketing. See *Hearing on Elec. Commc'ns Privacy Act Reform & the Revolution in Location Based Techs. & Servs. Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties, S. Comm. on the Judiciary,* 111th Cong. (June 24, 2010), (Written Testimony of Professor Matt Blaze at 11) ("Maintaining such detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect this trend to continue as part of the natural progression of technology.") *available at* http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf

Even if the information the government requested were not available from MetroPCS today, there is no way to tell whether that the information will be available tomorrow. Judge Smith addressed whether users of cell phones have a reasonable expectation of privacy in their location data, and determined that, under current capabilities and as technology exists now and is developing, location data acquisition intrudes on reasonable expectations of privacy. That approach was perfectly appropriate under Fourth Amendment doctrine. *See United States v. Kyllo,* 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."); *see also id.* at 40 (rejecting the idea that the constitutionality of the

surveillance should be judged on the basis of what occurred in the case at bar, and instead requiring courts to "take the long view" and give "clear specification of those methods of surveillance that require a warrant").

In addition, to dismiss the constitutional concern on the grounds the government is willing to amend its application to exclude that information it considers most intrusive would risk that the targeted providers would furnish that intrusive information nevertheless. In the absence of a legal directive, there is no reason for providers to filter location data to ensure that they deliver only that which the government requests. *See* Gidari, Jr., *Keynote Address*, 41 U.S.F. L. Rev. at 549 ("[u]nder every pen register order implemented, the government gets location. . . . The location information is just flowing as part of the solution."); *see also id*. at 550 (Service providers "are paying a fortune for the CALEA hardware and software, and they are not paying to filter it further.").

The government's argument that its limited request for information insulates that request from Fourth Amendment scrutiny boils down to a claim that its agents in the field may be trusted to protect Fourth Amendment rights through self-restraint. Law enforcement agents may not avoid the application of the Fourth Amendment by asserting that they themselves will limit their review of location data and that they may do so without meaningful judicial oversight. *Katz v. United States*, 389 U.S. 347, 356 (1967) (requiring that restraints on investigating agents be imposed "by a judicial officer" and not "by the agents themselves.").

CONCLUSION

Location data may provide an essential tool to government agents engaged in law enforcement. Just as with wiretapping, video surveillance, and conventional searches, however, acquisition of location information must be subject to Fourth Amendment safeguards, because

users have a reasonable expectation of privacy in their location data, whether the data is prospective or historical. When government agents acquire location data, they do so in a manner that is hidden, intrusive, indiscriminate and continuous and therefore must be subject to at least the protections of a warrant based on a showing of probable cause. Neither a third party rule nor the fact that location data disclosure is compelled obviates the warrant requirement. Magistrate Judge Smith did not abuse his discretion in supplementing the government's submission. He properly denied the government's requests for location data without a warrant based on probable cause and his opinion should be affirmed.

Respectfully submitted

Date January 14, 2010 s/ Susan Freiwald

Susan Freiwald
Professor of Law
University of San Francisco
School of Law
2130 Fulton Street
San Francisco, CA 94117
NY2557627
Phone: (415) 422-6467
E-mail: freiwald@usfca.edu

CERTIFICATE OF SERVICE

I hereby certify that on January 14, 2010, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification to the appropriate parties.

s/ Susan Freiwald